9110-9B

DEPARTMENT OF HOMELAND SECURITY

48 CFR Parts 3001, 3002, 3004 and 3052

Docket No. DHS-2017-0006

RIN 1601-AA76

Homeland Security Acquisition Regulation (HSAR); Safeguarding of Controlled Unclassified Information (HSAR Case 2015-001)

AGENCY: Office of the Chief Procurement Officer, Department of Homeland Security (DHS).

ACTION: Proposed rule.

SUMMARY: DHS is proposing to amend the Homeland Security Acquisition Regulation (HSAR) to modify a subpart, remove an existing clause and reserve the clause number, update an existing clause, and add a new contract clause to address requirements for the safeguarding of Controlled Unclassified Information (CUI).

DATES: Comments on the proposed rule should be submitted in writing to one of the addresses shown below on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], to be considered in the formation of the final rule.

ADDRESSES: Submit comments identified by HSAR Case 2015-001, Safeguarding of Controlled Unclassified Information, using any of the following methods:

- Regulations.gov: *http://www.regulations.gov*.

Submit comments via the Federal eRulemaking portal by entering "HSAR Case 2015–001" under the heading "Enter Keyword or ID" and selecting "Search." Select the link "Submit a Comment" that corresponds with "HSAR Case 2015-001." Follow the

instructions provided at the "Submit a Comment" screen. Please include your name, company name (if any), and "HSAR Case 2015–001" on your attached document.

- Fax: (202) 447-0520
- Mail: Department of Homeland Security, Office of the Chief Procurement Officer, Acquisition Policy and Legislation, ATTN: Ms. Shaundra Duggans, 245 Murray Drive, Bldg. 410 (RDS), Washington, DC 20528.

Comments received generally will be posted without change to *http://www.regulations.gov*, including any personal information provided. To confirm receipt of your comment(s), please check *www.regulations.gov*, approximately two to three days after submission to verify posting (except allow 30 days for posting of comments submitted by mail).

FOR FURTHER INFORMATION CONTACT: Ms. Shaundra Duggans, Procurement Analyst, DHS, Office of the Chief Procurement Officer, Acquisition Policy and Legislation at (202) 447-0056 or email *HSAR@hq.dhs.gov*. When using email, include HSAR Case 2015-001 in the "Subject" line.

SUPPLEMENTARY INFORMATION:

I. Background

The purpose of this proposed rule is to implement adequate security and privacy measures to safeguard Controlled Unclassified Information (CUI) and facilitate improved incident reporting to DHS. This proposed rule does not apply to classified information. These measures are necessary because of the urgent need to protect CUI and respond appropriately when DHS contractors experience incidents with DHS information. Recent high-profile breaches of Federal information further demonstrate the need to ensure that

information security protections are clearly, effectively, and consistently addressed in contracts. This proposed rule strengthens and expands existing HSAR language to ensure adequate security for CUI that is accessed by contractors; collected or maintained by contractors on behalf of an agency; and/or for Federal information systems that collect, process, store or transmit such information. The proposed rule identifies CUI handling requirements as well as incident reporting requirements, including timelines and required data elements. The proposed rule also includes inspection provisions and post-incident activities and requires certification of sanitization of Government and Government-Activity related files and information. Additionally, the proposed rule requires that contractors have in place procedures and the capability to notify and provide credit monitoring services to any individual whose Personally Identifiable Information (PII) or Sensitive PII (SPII) was under the control of the contractor or resided in the information system at the time of the incident.

This rule addresses the safeguarding requirements specified in the Federal Information Security Modernization Act (FISMA) of 2014 (44 U.S.C. 3551, *et seq.*), Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[1], relevant National Institutes of Standards and Technology (NIST) guidance, Executive Order 13556, *Controlled Unclassified Information*[2] and its implementing regulation at 32 CFR Part 2002[3], and the following OMB Memoranda: M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable*

[1] OMB Circular A-130 *Managing Information as a Strategic Resource* is accessible at https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.
[2] Executive Order 13556 *Controlled Unclassified Information* is accessible at https://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf
[3] 32 CFR Part 2002 is accessible at https://www.gpo.gov/fdsys/pkg/FR-2016-09-14/pdf/2016-21665.pdf

Information; M-14-03, *Enhancing the Security of Federal Information and Information Systems*; and Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management as identified in various OMB Memoranda.[4] Ongoing efforts by OMB and DHS with regard to implementation of FISMA, such as the issuance of Binding Operational Directives, and DHS implementation of the CUI program, may require future HSAR revisions in this area. DHS intends to harmonize the HSAR to be consistent with the requirements of these ongoing efforts.

II. Discussion and Analysis

This proposed rule is part of a broader initiative within DHS to (1) ensure contractors understand their responsibilities with regard to safeguarding controlled unclassified information (CUI); (2) contractor and subcontractor employees complete information technology (IT) security awareness training before access is provided to DHS information systems and information resources or contractor-owned and/or operated information systems and information resources where CUI is collected, processed, stored or transmitted on behalf of the agency; (3) contractor and subcontractor employees sign the DHS RoB before access is provided to DHS information systems, information resources, or contractor-owned and/or operated information systems and information resources where CUI is collected, processed, stored or transmitted on behalf of the agency; and (4) contractor and subcontractor employees complete privacy training before accessing a Government system of records; handling personally identifiable information

[4] These memoranda include M-03-19, M-04-25, M-05-15, M-06-20, M-07-19, M-08-212, M-09-29, M-10-15, M-11-33, M-12-20, M-14-04, M-15-01, M-16-03, and M-16-04. These memoranda can be accessed at: https://www.whitehouse.gov/omb/memoranda_default.

(PII) and/or sensitive PII information; or designing, developing, maintaining, or operating a system of records on behalf of the Government.

DHS is proposing to amend and expand an existing HSAR subpart. This proposed rule would (1) add new definitions; (2) clarify the applicability of the subpart; (3) remove an existing clause and reserve the clause number; (4) revise an existing clause; and (5) add a new clause to implement expanded safeguarding requirements and identify new policies for incident reporting, incident response, notification and credit monitoring. Each of these proposed changes are described in detail below.

(1) DHS is proposing to revise subpart 3002.101, Definitions, to define "adequate security," "controlled unclassified information," "Federal information," "Federal information system," "handling," "information resources," "information security," and "information system," " and remove the definition of sensitive information. The definition of the terms "adequate security," "Federal information," and "Federal information system" is taken from OMB Circular A-130, *Managing Information as a Strategic Resource*. The definition of controlled unclassified information is taken from its implementing regulation at 32 CFR Part 2002. The definition of "handling" was developed based upon a review of definitions for the term developed by other Federal agencies. The definition for the term "information security" is taken from FISMA 2014 (44 U.S.C. 3552(b)(3)) and the definitions for the terms "information resources" and "information system" are taken from 44 U.S.C. 3502(6) and 44 U.S.C. 3502(8) respectively. The definition of "sensitive information" is removed because it is being replaced with "controlled unclassified information" consistent with Executive Order 13556 and its implementing regulation at 32 CFR Part 2002. This rule also adds five (5)

new categories/subcategories of CUI titled Homeland Security Agreement Information, Homeland Security Enforcement Information, Operations Security Information, Personnel Security Information, and Sensitive Personally Identifiable Information for consistency with NARA's CUI regulation (32 CFR Part 2002). The definitions of these terms are needed because these terms appear in the new proposed clause at 3052.204-7X, *Safeguarding of Controlled Unclassified Information*.

(2) DHS is proposing to revise subpart 3004.470, Security requirements for access to unclassified facilities, Information Technology resources, and sensitive information, to change the title of the subpart and to clarify the applicability of the subpart to the acquisition lifecycle. The title of the subpart would be changed to "Security requirements for access to unclassified facilities, information resources, and controlled unclassified information" and a new subsection for definitions would be added under the subpart. Accordingly, the subsections would be renumbered as follows: 3004.470-1 Scope, 3004.470-2 Definitions, 3004.470-3 Policy, and 3004.470-4 Contract Clauses. Originally, the title of this subpart contained the term "information technology resources;" however, this term is inconsistent with 44 U.S.C. 3502(6) which defines the term "information resources." Subsection 3004.470-1, Scope, would be amended for consistency in terminology and to make clear the applicability of the subpart to the acquisition lifecycle. Subsection 3004.470-2, Definitions, would be added to define the term "incident." The definition for "incident" is taken from FISMA 2014 (44 U.S.C. 3552(b)(2)). This term could not be defined at 3002.1, Definitions, because the meaning of the term "incident" in this subpart differs from the meaning it is given in other parts of the HSAR. Additionally, this definition is needed because this term appears in the clause

at 3052.204-7X, *Safeguarding of Controlled Unclassified Information*. Subsection 3004.470-3, Policy, would be revised to (a) remove explicit references to Departmental policies and procedures to safeguard CUI that are subject to change and provide a public facing link for which these policies and procedures can be accessed and (b) make clear the requirements for completion of security forms and background investigations for contractor employees that require recurring access to Government facilities or CUI. Subsection 3004.470-4, Contract Clauses, would be revised to remove reference to 3052.204-70, Security Requirements for Unclassified Information Technology Resources and identify the applicability of the clause at 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, to solicitations, contracts, and subcontracts.

(3) Clause 3052.204-70, Security Requirements for Unclassified Information Technology Resources, would be removed and the clause number reserved. This change is necessary because the addition of the clause at 3052.204-7X *Safeguarding of Controlled Unclassified Information* eliminates the need for this clause.

(4) A new clause at 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, would be added to ensure adequate protection of CUI. The new clause adds definitions and identifies CUI handling requirements, Authority to Operate requirements, incident reporting and response requirements, PII and SPII notification requirements, credit monitoring requirements, sanitization of Government and Government-Activity related files and information requirements, other reporting requirements, and subcontract requirements. Each of these requirements is described below.

(a) Definitions

This section would add definitions, which also appear in part at 3002.1 Definitions and 3004.470-2 Definitions, as follows: “adequate security,” “Controlled Unclassified Information,” “Federal information,” “Federal information system,” “handling,” “Homeland Security Agreement Information,” “Homeland Security Enforcement Information,” “incident,” “information resources,” “information security,” “information system,” “Operations Security Information,” “Personnel Security Information,” and “Sensitive Personally Identifiable Information.” The definitions of these terms are needed because these terms appear in 3052.204-7X, *Safeguarding of Controlled Unclassified Information.*

(b) Handling of Controlled Unclassified Information

This section sets forth specific requirements for contractors and subcontractors when handling CUI in order to better protect against the threat of persistent cyber-attacks and prevent the compromise of CUI, including PII. These requirements include being in compliance with the DHS policies and procedures in effect at the time of contract award. These policies and procedures are located on a public website titled DHS Security and Training Requirements for Contractors which can be accessed via http://www.dhs.gov/dhs-security-and-training-requirements-contractors. This website identifies Departmental policies and procedures that contractors must comply with related to personnel security, information security, IT security, and privacy. The website also identifies and provides contractors with access to IT security awareness and privacy training. The policies and training requirements contained on this website are existing requirements that DHS routinely includes in the terms and conditions of its contracts, some of which are pre-existing through HSAR 3052.204-70 *Security Requirements for*

Unclassified Information Technology Resources and 3052.204-71 *Contractor Employee Access*. Part of the intent of this proposed rulemaking is to increase transparency by consolidating these existing requirements in a single location that is easily accessible by the public. Changes to these policies and procedures will be reflected on the website and changes that impact contract performance will be communicated to the contractor by the Government.

Handling requirements also include not using or redistributing any CUI collected, processed, stored, or transmitted by the contractor, except as specified in the contract and not maintaining SPII in the contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions. DHS believes that maintaining SPII in the contractor's invoicing, billing, and other recordkeeping systems creates unnecessary risk of compromise and is not otherwise needed to achieve contract administration functions. DHS welcomes comments regarding whether other categories of CUI should be similarly excluded from a contractor's invoicing, billing, and other recordkeeping systems. Through these and other requirements set forth in the proposed clause and discussed in detail in the following sections, the Department believes that contractors and subcontractors will provide adequate security from the unauthorized access and disclosure of CUI.

(c) Authority to Operate

FISMA defines a comprehensive framework for ensuring the protection of Government information, operations and assets against natural or man-made threats. This section sets forth information security requirements contractors operating a Federal information system must meet prior to collecting, processing, storing, or transmitting CUI in that information system as required by FISMA and set forth in NIST Special Publication 800-

53, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*. The requirements include completing the security authorization process, including the preparation of security authorization package and obtaining an independent assessment; renewal of the security authorization; security review; and Federal reporting and continuous monitoring.[5]

Security authorization involves comprehensive testing and evaluation of security features (also known as controls) of an information system. It addresses software and hardware security safeguards; considers procedural, physical, and personnel security measures; and establishes the extent to which a particular design (or architecture), configuration, and implementation meets a specified set of security requirements throughout the life cycle of the information system. It also considers procedural, physical, and personnel security measures employed to enforce information security policy. The security authorization package includes a Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, and Security Assessment Report. These documents are used to record the results of the security authorization process and provide evidence that the process was followed correctly. A Federal information system, which includes a contractor information system operating on behalf of an agency, must be granted an Authority to Operate (ATO) before it is granted permission to collect, process, store, or transmit CUI. The ATO is the official management decision given by a senior organizational official to authorize operation of

[5] DHS is aware that NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, was released in June 2015 to provide federal agencies with recommended requirements for protecting the confidentiality of Controlled Unclassified Information on non-Federal information systems; however, the information system security requirements in this proposed rulemaking are focused on Federal information systems, which include contractor information systems operating on behalf of an agency. Consistent with 32 CFR Part 2002, these information systems are not subject to the requirements of NIST Special Publication 800-171.

an information system based on the implementation of an agreed-upon set of security controls.

The independent assessment is used to validate the security and privacy controls in place for the information system prior to submission of the security authorization package to the Government for review and acceptance. Once an ATO is accepted and signed by the Government, it is valid for three (3) years and must be renewed at that time unless otherwise specified in the ATO letter. The Government uses random security reviews as an additional level of verification to ensure security controls are in place, enforced and operating effectively. The contractor shall afford access to DHS, the Office of the Inspector General, other Government organizations, and contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract to conduct security reviews. In addition, contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by OMB on an annual basis and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan.[6] The plan is updated annually to reflect any new or revised reporting requirements from OMB.

(d) Incident Reporting

This section sets forth incident reporting requirements for contractors and subcontractors when reporting known or suspected incidents, including known or suspected incidents that involve PII and/or SPII. The incident reporting requirements

[6] The Fiscal Year 2015 DHS Information Security Performance Plan can be found at: http://www.dhs.gov/dhs-security-and-training-requirements-contractors.

described in this section allow the Department to gather the information necessary to formulate an effective incident response plan for incident mitigation and resolution. These requirements include: reporting all known or suspected incidents to the Component Security Operations Center and notifying the contracting officer and contracting officer's representative of the incident; reporting known or suspected incidents that involve PII or SPII within one hour of discovery and all other incidents within eight hours of discovery; encrypting CUI using FIPS 140-2 Security Requirements for Cryptographic Modules and refraining from including CUI in the subject or body of any email; providing additional data elements when reporting incidents involving PII or SPII; and making clear that an incident shall not, by itself, be interpreted as evidence that the contractor failed to provide adequate information security safeguards for CUI.

The timing for reporting incidents involving PII or SPII is consistent with OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information. The timing for reporting incidents unrelated to PII or SPII was derived from existing Departmental policy for reporting incidents related to other categories of CUI such as CVI, Protected Critical Infrastructure Information (PCII), and Sensitive Security Information (SSI). Controlled unclassified information is required to be excluded from the subject or body of an email and encrypted to prevent further compromise of the information when reporting incidents. The additional data elements required when reporting incidents involving PII or SPII are needed to assist in the Department's understanding of the incident and aid in an effective response. DHS also wants to encourage industry to timely report incidents to the Department by making it

clear that such reporting does not automatically mean the contractor has failed to provide adequate security or otherwise meet the requirements of the contract.

(e) Incident Response

This section identifies incident response requirements and activities. Incident response activities such as inspections, investigations, forensic reviews, etc. are used to quickly assess, remediate and protect CUI and are conducted whenever an incident is reported to DHS. The goal of these activities is to determine what data was or could have been accessed by an intruder, build a timeline of intruder activity, determine methods and techniques used by the intruder, find the initial attack vector, identify any features/aspects in the information security protections, and provide remediation recommendations to restore the protection of the data. Incident response activities may also include contract compliance analyses.

(f) PII and SPII Notification Requirements

This section sets forth the notification procedures and capability requirements for Contractors when notifying any individual whose PII and/or SPII was under the control of the Contractor or resided in the information system at the time of the incident. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer utilizing the DHS Privacy Incident Handling Guidance. When appropriate, notification of those affected and/or the public allows those individuals affected by the incident the opportunity to take steps to help protect themselves. Such notification is also consistent with the "openness principle" of the Privacy Act which calls for agencies to inform individuals about how

their information is being accessed and used, and may help individuals mitigate the potential harms resulting from an incident.

The Department realizes that there are existing state notification laws that industry must also follow. Therefore, DHS welcomes comments regarding the impact, if any, that existing state notification laws will have on industry's ability to comply with this notification requirement.

(g) Credit Monitoring

This section sets forth the requirement that the contractor, when appropriate, is required to provide credit monitoring services, including call center services, if directed by the Contracting Officer, to any individual whose PII or SPII was under the control of the contractor, or resided in the information system, at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring is a commercial service that can assist individuals in early detection of instances of identity theft. Credit monitoring services notify individuals of changes that appear in their credit report, such as creation of new accounts, changes to their existing accounts or personal information, or new inquiries for credit. Such notification affords individuals the opportunity to take steps to minimize any harm associated with unauthorized or fraudulent activity. The section is only applicable when an incident involves PII or SPII.

The Department deliberately made the provision of notification and credit monitoring services independent from an assessment of fault or lack of compliance with the contract terms and conditions. In accordance with OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable

Information, agencies have the responsibility to notify individuals whose PII or SPII may have been compromised without unreasonable delay. This notification has often been delayed while detailed forensic analysis and contract compliance inspections are occurring. Under this new provision, notification and credit monitoring, when appropriate, will occur more rapidly as it is not dependent upon any determination of contractor fault or noncompliance. DHS is also aware that sophisticated cyber-attacks can occur despite compliance with contract requirements. In these instances, even though there is no contractor noncompliance, there may still be a need to notify individuals and provide credit monitoring services. Additionally, DHS wants to emphasize that the provisions for notification and credit monitoring services are only applicable when (1) contractor and/or subcontractor employees may have access to PII/SPII or (2) information systems are used to collect, process, store, or transmit PII/SPII on behalf of the agency. DHS is considering broadening the credit monitoring requirement to include identity protection, identity restoration, and related services. DHS welcomes comments regarding the impact, if any, of this change.

(h) Certificate of Sanitization of Government and Government-Activity Related Files and Information

Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise identified in the contract, the Contractor must return all CUI to DHS or destroy it physically or logically as identified in the contract. This destruction must conform to the guidelines for media sanitization contained in NIST SP-800-88, Guidelines for Media Sanitization. Further, the contractor must certify and confirm sanitization of media using the template provided in Appendix G of the publication.

(i) Other Reporting Requirements

The purpose of this section is to make clear that the requirements of this clause do not rescind the Contractor's responsibility for compliance with other applicable U.S. Government statutory or regulatory requirements that may apply to its contract(s).

(j) Subcontracts

This section requires that contractors insert the clause at 3052.204-7X *Safeguarding of Controlled Unclassified Information* in all subcontracts and require subcontractors to include this clause in all lower-tier subcontracts. The requirements of this clause are applicable to all contractors and subcontractors that (1) will have access to CUI; (2) collect or maintain CUI on behalf of the agency; or (3) operate Federal information systems, including contractor information systems operated on behalf of the agency, to collect, process, store, or transmit CUI.

(5) Clause 3052.212-70, *Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items*, would be revised to remove 3052.204-70, *Security Requirements for Unclassified Information Technology Resources*; identify Alternate II as an option under subparagraph (b) of 3052.204-71 *Contractor Employee Access*; and add 3052.204-7X *Safeguarding of Controlled Unclassified Information* under subparagraph (b) of the clause. The addition of 3052.204-7X *Safeguarding of Controlled Unclassified Information* eliminates the need for 3052.204-70 Security Requirements for Unclassified Information Technology Resources. Because of this 3052.204-70 would be removed and the clause number reserved. Alternate II to 3052.204-71 was inadvertently omitted as an option under the listing of clauses and alternates available for selection under 3052.212-70. This addition corrects that omission. Subparagraph (b) of 3052.212-

70 would also be amended to add 3052.204-7X *Safeguarding of Controlled Unclassified Information* because the requirements of these clauses are applicable to the acquisition of commercial items.

(6) Other considerations. DHS is considering making changes to subpart 3004.470-3, Contract Clauses, and the clause at 3052.204-71, Contractor Employee Access. These changes would harmonize the text of the clause with the requirements of the final version of 3052.204-7X *Safeguarding of Controlled Unclassified* Information by removing outdated and/or unnecessary definitions (i.e., sensitive information and information technology resources); renumbering the paragraphs of the clause as a result of the removal of the definitions for the terms "sensitive information" and "information technology resources"; and making clear in the prescription for the clause the need for information security regardless of the setting, including educational institutions and contractor facilities. DHS believes that the protection of CUI is paramount regardless of where the information resides. DHS is also seeking comment on making the clause at 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, applicable to all services contracts. DHS believes this broader applicability would ensure that contractors are aware of the Government's requirements related to CUI. In addition, the Government believes that the requirements of the clause are written in such a way that they would be self-deleting when they are not applicable to a solicitation or contract. DHS welcomes comments regarding the impact, if any, on including 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, in all services contracts. DHS also welcomes comments and feedback on industry's understanding of the concept of self-deleting and if

the use of alternates to 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, is needed to ensure proper understanding and application of the clause.

III. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action and, therefore, was subject to review under Section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is not a major rule under 5 U.S.C. 804.

This proposed rule addresses the safeguarding requirements specified in the FISMA, OMB Circular A-130, *Managing Information as a Strategic Resource*, relevant NIST guidance, Executive Order 13556, *Controlled Unclassified Information* and its implementing regulation at 32 CFR Part 2002, and multiple OMB Memoranda. DHS considered both the costs and benefits associated with the requirements of proposed clause *Safeguarding of Controlled Unclassified Information*, specifically those requirements believed to be of most import to industry such as the requirement to: obtain an independent assessment, perform continuous monitoring, report all known and suspected incidents, provide notification and credit monitoring services in the event an incident impacts PII, document sanitization of Government and Government-activity-related files and information, as well as ensure overall compliance with the requirements

of the proposed clause.

To determine the estimated costs of these requirements DHS requested cost information from multiple vendors whose contracts with DHS include requirements similar to this proposed rule; obtained cost input from the Federal Risk and Authorization Management Program (FedRAMP), for which DHS is a participant; reviewed the Congressional Budget Office (CBO) Cost Estimate for the Personal Data Protection and Breach Accountability Act of 2011; reviewed pricing from the General Service Administration's (GSA) recently awarded Identity Protection Services (IPS) blanket purchase agreements (BPAs); and reviewed internal price data from DHS's Managed Compliance Services and notification and credit monitoring services contracts. These activities identified that: (1) the cost of an independent assessment can range from $30,000 to $150,000 with an average cost of $112,872; (2) the equipment costs to perform continuous monitoring can range from $76,340 to $350,000 with an average cost of $213,170 while the labor costs to perform continuous monitoring can range from $47,000 to $65,000 for an average cost of $55,674; (3) the cost of reporting an incident to DHS ranges between $500 and $1,500 per incident; (4) the cost of notifying individuals that there has been an incident with their PII ranges from $1.03 to $4.60 per person; (5) the cost of credit monitoring services range between $60 and $260 per person; (6) a specific cost for the certificate of sanitization of Government and Government-Activity-Related files and information cannot be determined as the methods of sanitization vary widely depending on the categorization of the system and the media on which the data is stored; and (7) costs associated with Full-time Equivalent (FTE) oversight of the requirements of proposed clause *Safeguarding of Controlled Unclassified Information*

ranges from $65,000 to $324,000. Detailed information on how DHS arrived at these costs and ranges is provided below.

There are a multitude of benefits associated with the requirements of proposed clause *Safeguarding of Controlled Unclassified Information*. These benefits impact both DHS and contractors with which it conducts business. Benefits related to specific provisions of the proposed clause are addressed below; however, it is important to note the overarching benefit of transparency. While several of the requirements of the proposed clause have been routinely included in DHS contracts (e.g., Authority to Operate, notification, and credit monitoring), this proposed rulemaking standardizes the applicability of these requirements and makes clear to contractors considering doing business with DHS the standards and requirements to which they will be held as it relates to the (1) handling of the Department's CUI, (2) security requirements when such information will be collected or maintained on behalf of the agency or collected, processed, stored, or transmitted in a Federal information system, including contractor information systems operating on behalf of the agency, and (3) potential notification and credit monitoring requirements in the event of an incident that impacts personally identifiable information (PII) and/or sensitive PII (SPII). The current lack of standardization and transparency has been point of contention for industry and a common concern raised when DHS has requested feedback from industry.

OVERVIEW OF COSTS:

Independent Assessment

DHS is proposing that vendors obtain an independent assessment to validate the security and privacy controls in place for an information system prior to submission of

the security authorization package to the Government for review and acceptance. In general, when assessing compliance with a standard or set of requirements, there are three alternatives: (1) first party attestation or self-certification, (2) second party attestation (i.e., internal independent), or (3) third party attestation. While the first two options may be considered the least economically burdensome, third party attestation is an accepted best practice in commercial industry as objectivity increases with independence. DHS is proposing to require that vendors obtain an independent assessment from a third party to ensure a truly objective measure of an entity's compliance with the requisite security and privacy controls. Recent high-profile breaches of Federal information further demonstrate the need for Departments, agencies, and industry to ensure that information security protections are clearly, effectively, and consistently addressed and appropriately implemented in contracts. Additionally, the benefits of using a third party to perform an independent assessment also extend to the contractor as the contractor can use the results of the independent assessment to demonstrate its cybersecurity excellence for customers other than DHS.

The cost of an independent assessment varies widely depending upon the complexity of the information system, the categorization of the information system (low, moderate, or high impact), and the sophistication of the contractor. Additionally, DHS does not have a mechanism to track the costs of independent assessments performed under its contracts. Because of the multiple factors that influence the cost of an independent assessment and lack of a tracking mechanism for associated costs, DHS is unable to identify with specificity the costs of implementing this requirement. As such, we sought to identify a range of costs based on the actual data we were able to access.

DHS performed the following activities to obtain this data:

- Requested cost information from multiple vendors whose contracts with DHS require an independent assessment as part of the security authorization process;
- Obtained cost input from FedRAMP, for which DHS is a participant, as the program requires cloud service providers to obtain an independent assessment from a Third Party Assessment Organization; and
- Reviewed internal data from DHS's Managed Compliance Services contract. DHS uses this contract to perform internal independent assessments.

The cost information received from DHS vendors ranged from $30,000 to $123,615. The vendors whose costs were on the higher end of this range included costs for the independent party as well as internal labor costs associated with performing the independent assessment whereas the vendor on the low end of the spectrum did not. FedRAMP data indicates the estimated costs on an independent assessment to be approximately $150,000 while costs under DHS's internal contract for this service ranges between $35,000 and $45,000. When considering the data from DHS's internal contract for independent assessment services, it is important to note that these figures do not capture the labor costs of the Government employees involved in the process as the Government does not typically track the costs incurred for services performed by its own workforce. Because of this, it is both anticipated and expected that contractor costs for independent assessments will exceed the costs the Government incurs as contractor costs typically include not only the cost of the independent third party but also internal labor costs to facilitate the independent assessment and resolve any resultant findings.

Based on the above data points, the cost of an independent assessment can range from $30,000 to $150,000 or an average cost of $112,872. Because it seems likely that most vendors will have to account for necessary staff time, the average cost was developed by averaging only those cost estimates that included both internal and external labor costs. Neither the range nor the average cost identified is absolute as there are multiple factors that influence the cost of this service. Internal historical data indicates it takes approximately 162 labor hours to complete and independent assessment. This adds to the variance as the costs are dependent upon the labor categories and rates used to perform the assessment. Also, it is important to note that the assessment is required to be performed by an independent party. As such, the actual cost of the assessment is largely dependent upon agreements that the contractor is responsible for negotiating. Contractors with preexisting relationships with entities that perform independent assessments may be able to obtain more competitive pricing. Contractors new to this requirement may not. DHS welcomes comments from industry regarding the estimated costs associated with compliance with the requirement to obtain an independent assessment.

Continuous Monitoring

Proposed clause *Safeguarding of Controlled Unclassified Information* requires that contractors operating Federal information systems, which includes contractor information systems operating on behalf of the Government, or maintaining or collecting information on behalf of the Government, comply with information system continuous monitoring requirements. Continuous monitoring is not a new requirement for DHS contractors. Existing HSAR clause 3052.204-70, *Security Requirements for Unclassified Information Technology Resources*, requires contractors to comply with DHS Sensitive

System Policy Publication 4300A. This publication and its implementing guidance addresses continuous monitoring requirements. DHS is seeking to be more clear and transparent with contractor requirements by expressly identifying this requirement in proposed clause *Safeguarding of Controlled Unclassified Information*.

The costs associated with continuous monitoring are not fixed and can vary widely. For example, a contractor that has previously gone through DHS's security authorization process is more likely to have in place the hardware, software, and personnel to perform continuous monitoring. In this instance, the costs associated with performing this requirement would be lower than a contractor who does not have preexisting hardware, software, and personnel in place to satisfy these requirements.

Because of the multiple factors that influence the cost of continuous monitoring, DHS is unable to identify with specificity the costs of implementing this requirement. As such, we sought to identify a range of costs based on the actual data we were able to access. DHS performed the following activities to obtain this data:

- Requested cost information from multiple vendors whose contracts with DHS include similar continuous monitoring requirements; and
- Reviewed internal historical data.

The cost information received from DHS vendors ranged from $65,000 to $397,000. Vendors on the lower end of this range already had the hardware and software in place to perform continuous monitoring as the costs proposed only include labor. Alternatively, the vendors on the higher end of this range documented costs associated with hardware, software, and labor. For example, the cost breakdown from the vendor that reported costs of $397,000 included a one-time equipment fee of $350,000 and

annual labor costs of $47,000. Alternatively, the vendor that submitted costs of $65,000 only proposed labor costs and is using preexisting hardware and software to perform continuous monitoring.

A review of internal historical data indicates the cost of continuous monitoring ranges from $6,000 to $18,000. It is important to note that the internal historical data assumes the vendor has the appropriate tools to perform continuous monitoring (e.g., the ability to scan their assets) and does not include costs for the labor required to support continuous monitoring activities. It is both anticipated and expected that in many instances contractor costs for continuous monitoring will exceed the costs the Government incurs for the same service as contractor costs include the costs of hardware/software to perform continuous monitoring as well as labor costs to support continuous monitoring activities.

Using the above data points, the equipment costs to perform continuous monitoring can range from $76,340 to $350,000 with an average cost of $213,170. The average cost was developed by averaging the equipment costs received. Alternatively, labor costs to perform continuous monitoring can range from $47,000 to $65,000 for an average cost of $55,674. The average cost was developed by averaging the labor costs received. Please note these ranges and average costs are not absolute as the costs associated with continuous monitoring vary based on the tools (i.e., hardware or software) and methods (e.g., internal staff, contractor support, new hires) the contractor uses to implement the continuous monitoring requirements. The Government anticipates costs will decline over time as contractors become more sophisticated and build the necessary infrastructure to support this activity. DHS welcomes comments from industry

regarding the estimated costs associated with compliance with the requirement to perform continuous monitoring.

Incident Reporting

This proposed rule requires contractors to report known or suspected incidents that involve PII or sensitive PII (SPII) within one hour of discovery and all other incidents (i.e., those incidents impacting any other category of CUI) within eight hours of discovery. DHS specifically included language in the regulatory text stating that an incident shall not, by itself, be interpreted as evidence that the contractor has failed to provide adequate information security safeguards for CUI, or has otherwise failed to meet the requirements of the contract. This language was added because DHS understands that sophisticated cyber-attacks can occur despite compliance with contract requirements.

The cost to prepare and report an incident to DHS varies based on the type(s) of information impacted by the incident and the complexity of the incident. Proposed clause *Safeguarding of Controlled Unclassified Information* requires incidents to be reported to the Component Security Operations Center (SOC), or the DHS Enterprise SOC if the Component SOC is unavailable, in accordance with 4300A Sensitive Systems Handbook Attachment F Incident Response. However, if PII is impacted by the incident, the contractor must provide additional information in its incident report. Also, for incidents that impact multiple systems or multiple components of a system, it may take the contractor more resources (e.g., time) to obtain the some of the data points that are required to be provided when reporting an incident.

To determine the cost of preparing and reporting an incident, DHS performed the following activities:

- Requested cost information from multiple vendors whose contracts with DHS include similar incident reporting requirements; and
- Reviewed internal historical data.

It was difficult to use the information submitted by the vendors queried to establish an estimated cost. The information provided either included both incident reporting and incident response (i.e., investigation and remediation activities) or annual training and testing requirements. Because of this we had to rely on internal historical data to establish an estimate solely responsive to the incident reporting requirements identified in the proposed clause. This data indicates the estimated cost of reporting an incident to DHS ranges between $500 and $1,500 per incident. DHS estimates that 822 vendors are subject to the requirements of this proposed rule and that each vendor may report up to one known or suspected incident per year for a total estimated cost range of $411,000 to $1,233,000. DHS welcomes comments from industry regarding the estimated costs associated with incident reporting.

Notification and Credit Monitoring

In the event of an incident that impacts PII/SPII, it may be necessary to perform certain incident response activities such as notification and credit monitoring. Contractors should not assume that all incident response activities will take place when a known or suspected incident is reported to DHS as the determination on the appropriate incident response activities is based upon investigation of the known or suspected incident. DHS uses a deliberative process to investigate and determine if an incident has occurred. This process begins with the contractor's submission of an Incident report to the Component or DHS SOC. The SOC staff use the incident report information to

investigate and determine if an actual incident occurred. More often than not, an incident has not occurred and further incident response activities are not needed. If the SOC determines that incident has occurred, additional investigation and analyses happen to determine the nature and scope of the incident and US-CERT is engaged as necessary. If the incident involves PII/SPII, the Government will determine if notification and the provision of credit monitoring services is appropriate. DHS believes notification and credit monitoring, when appropriate, will occur more rapidly as the provision of these services is no longer dependent upon any determination of contractor fault or noncompliance.

To determine the cost of notifying individuals, DHS performed the following activities:

- Requested cost information from multiple vendors whose contracts with DHS include similar notification requirements;
- Reviewed pricing from DHS's department-wide contract for credit monitoring services;
- Reviewed the CBO Cost Estimate for the Personal Data Protection and Breach Accountability Act of 2011;
- Reviewed pricing from the GSA's recently awarded IPS BPAs; and
- Reviewed GSA's Professional Services Schedule, Financial and Business Solutions, Category 520 19 Data Breach Analysis.

The cost information we received from DHS vendors indicates that vendors price these requirements using different methods. One vendor bundled the cost of notification in its continuous monitoring costs while another bundled these costs as with those

associated with incident reporting. In these instances we are unable to determine which portion of the costs are associated with the notification requirements. The cost submitted by the one vendor that separately priced this requirement was $4.06 per person. The pricing for notification in the Department's internal contract for credit monitoring services is significantly lower than the costs proposed by DHS's vendors, i.e., $1.57 per person.

While the CBO report referenced above did not provide a cost estimate for notification, the following information was provided: "According to industry sources, the sensitive, personally identifiable information of millions of individuals is illegally accessed or otherwise breached every year. However, according to those sources, 46 states already have laws requiring notification in the event of a security breach. In addition, it is the standard practice of most businesses to notify individuals if a security breach occurs. Therefore, CBO estimates that the notification requirements would not impose significant additional costs on businesses."

GSA's IPS BPAs contain bundled fixed unit pricing for services that not only exceed the requirements of proposed clause *Safeguarding of Controlled Unclassified Information* (i.e., dedicated, branded website; identity restoration services; and identity theft insurance services) but also includes notification. As such, DHS is unable to determine which portion of the fixed unit price is applicable to notification services. A review of GSA's Professional Services Schedule indicates only two vendors with specific pricing for notification services. This includes the vendor for which DHS has a Department-wide contract for credit monitoring and notification services. Pricing for the other vendor is $0.54 per letter plus postage, i.e., $1.03. Based on this data, the cost of

notifying individuals that there has been an incident with their PII ranges from $1.03 to $4.60 per person. DHS welcomes comments from industry regarding the estimated costs associated with compliance with the requirement to provide notification services.

Proposed clause *Safeguarding of Controlled Unclassified Information* requires contractors to provide credit monitoring services, including call center services, if directed by the Contracting Officer, to any individual whose PII/SPII was under the control of the contractor, or resided in the information system, at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified.

The costs associated with this requirement vary depending on the method the contractor uses to provide services. For example, some contractors choose to satisfy this requirement through cyber insurance while others choose to subcontract these services with credit monitoring service providers. To estimate a cost for credit monitoring services, DHS performed the following activities:

- Requested cost information from multiple vendors whose contracts with DHS include similar credit monitoring requirements;
- Reviewed pricing from DHS's department-wide contract for credit monitoring services;
- Reviewed the CBO Cost Estimate for the Personal Data Protection and Breach Accountability Act of 2011; and
- Reviewed pricing from the General Service Administration's (GSA) recently awarded Identity Protection Services (IPS) blanket purchase agreements (BPAs).

The cost information we received from DHS vendors indicates that vendors satisfy these requirements using different methods. One vendor used cyber insurance while others satisfied this requirements through subcontracts with credit monitoring service providers. In instances where subcontracts are used, the pricing ranged from $61.71 to $260 per person. We assume that this variance in cost stems from the vendor's ability to negotiate favorable pricing with its subcontractors. It is also important to note that credit monitoring service providers frequently offer volume discounts that can lower the costs of services. However, all vendors under contracts with DHS may not able to capitalize on these discounts as the amount of PII provided to a contractor is based upon the services being provided and can vary greatly from contract to contract.

The pricing in the Department's internal contract for credit monitoring services is significantly lower than the costs proposed by DHS's vendors, i.e., $1.89 per person. It is important to note that DHS was able to obtain such favorable pricing because the cost of credit monitoring services are paid for everyone that receives notification of the incident without regard to their actual acceptance/request for credit monitoring. According to the CBO report referenced above, "[t]he cost of bulk purchases of the credit-monitoring or reporting services is about $60 per person according to credit industry professionals."

As it relates to GSA's IPS BPAs, the published price lists do not mirror the credit monitoring provisions of DHS's proposed clause *Safeguarding of Controlled Unclassified Information*. For example, the IPS BPAs contain bundled fixed unit pricing for services that exceed the requirements of the proposed clause (i.e., dedicated, branded website; identity restoration services; and identity theft insurance services). Additionally, the pricing includes volume discounts based on the number of individuals receiving

services. The prices ranged from $12.21 (per person per year if 10,000 - 24,999) to $38 (per person per year if more than 10,000).

Based on the aforementioned information, DHS believes the most likely costs for these services range between $60 and $260 per person. DHS welcomes comments from industry regarding the estimated costs associated with compliance with the requirement to provide credit monitoring. DHS also requests feedback from industry on how many individuals typically sign up for credit monitoring after being notified that an incident has occurred that impacts their PII/SPII?

Certificate of Sanitization

Proposed clause *Safeguarding of Controlled Unclassified Information* requires contractors to return all CUI to DHS and certify and confirm the sanitization of all Government and Government-Activity related files and information. Destruction must conform to the guidelines for media sanitization contained in NIST SP-800-88, Guidelines for Media Sanitization. The contractor is also required to use the template provided in NIST Special Publication 800-88, Guidelines for Media Sanitization, Appendix G when submitting the Certificate of Sanitization.

NIST SP 800-88 identifies the proper and applicable techniques and controls for sanitization and disposal decisions, considering the security categorization of the associated system's confidentiality. Applicable sanitization methods depend on the media in which the data is stored. Following sanitization, NIST SP 800-88 requires a certificate of media disposition to be completed for each piece of electronic media that has been sanitized. The proposed clause *Safeguarding of Controlled Unclassified Information* requires contractors to certify that applicable media have been sanitized

using the template provided in Appendix G of NIST SP 800-88. In short, this template states that a system or hardware has been sanitized of all information. The costs associated with media sanitization do not arise from completion of the template. The costs arise from the sanitization activities themselves. A specific cost cannot be provided as the methods of sanitization vary widely depending on the categorization of the system and the media on which the data is stored. DHS requests comments from industry regarding the estimated costs associated with compliance with the requirement to sanitize Government and Government-Activity-Related files and information.

Oversight and Compliance

As discussed above, the costs associated with oversight and compliance with the requirements contained in proposed clause *Safeguarding of Controlled Unclassified Information* are not easily quantifiable. Implementation costs stem directly from a vendor's pre-existing information security posture. Several vendors, particularly those operating in the IT space, have been complying with these requirements for years. In these instances, the vendors have the existing infrastructure (i.e., hardware, software, and personnel) to implement these requirements and implementation costs are lower. The same is also true for many vendors that provide professional services to the Government and use IT to provide those services. Alternatively, vendors with less experience and capability in this area will incur costs associated with procuring the hardware and software necessary to implement these requirements, as well as the labor costs associated with any new personnel needed to implement and oversee these requirements. Costs will vary depending on the hardware and software selected and the skill set each contractor requires in its employee(s) responsible for ensuring compliance with these requirements.

It is anticipated that these costs will be passed on to the Department, and that over time these vendors will become more sophisticated in this area and costs will decline. It is also important to note that the information security measures proposed in this rulemaking are quite similar to those industry already employs internal to their business operations. However, based on the feedback we received from vendors, the costs associated with FTE oversight of these requirements ranges from $65,000 to $324,000. This range is not absolute as it is entirely dependent upon the vendor's approach to oversight, i.e., a single individual, multiple personnel, and the seniority of the position, all of which directly impact costs. Also, it is important to note that requirements of this type are generally not priced as a separate line item and are typically captured in overhead estimates. As such, DHS does not have clear insight into the costs associated with this requirement. DHS welcomes comments from industry regarding the estimated costs associated with ensuring proper oversight and compliance with the requirements of proposed clause *Safeguarding of Controlled Unclassified Information*.

OVERVIEW OF BENEFITS:

Clear Notification of System Requirements

Feedback from industry has consistently indicated the need for transparency and clear and concise requirements as it relates to information security. The requirements of proposed clause *Safeguarding of Controlled Unclassified Information* is, in part, intended to satisfy this request. Previously information security requirements were either imbedded in a requirements document (i.e., Statement of Work, Statement of Objectives, or Performance Work Statement) or identified through existing HSAR clause 3052.204-70, *Security Requirements for Unclassified Information Technology Requirements*. This

approach (1) created inconsistencies in the identification of information security requirements for applicable contracts, (2) required the identification and communication of security controls for which compliance was necessary after contract award had been made, and (3) resulted in delays in contract performance.

Proposed clause *Safeguarding of Controlled Unclassified Information* substantially mitigates the concerns with DHS's previous approach. Through the Government provided Requirements Traceability to Matrix (RTM) contractors will know at the solicitation level the security requirements for which they must comply. The RTM identifies the security controls that must be implemented on an information system that collects, processes, stores, or transmits CUI and is necessary for the contractor to prepare its security authorization package. Clear identification of these requirements at the solicitation level affords contractors the ability to (1) assess their qualifications and ability to fully meet the Government's requirements, (2) make informed business decisions when deciding to compete on Government requirements, and (3) engage subcontractors, if needed, early in the process to enable them the ability to be fully responsive to the Government's requirements. Similarly, the Government benefits from clear identification of its requirements. Presumably, proposals/quotations will be submitted by contractors fully qualified and able to meet the requirements of the effort. During the evaluation phase of a procurement, the Government will be able to assess a contractor's information security posture and ability to comply with the requirements of the RTM. Such an evaluation should reduce post-award delays in contractor performance and mitigate the need to reissue solicitations as a result of a contractor's inability to comply with mandatory security requirements.

Improved Notification to the Public Regarding Data Breaches

Proposed clause *Safeguarding of Controlled Unclassified Information* requires contractors to have in place procedures and the capability to notify any individual whose PII) and/or SPII was under the control of the contractor or resided in the information system at the time of an incident no later than 5 business days after being directed to notify individuals, unless otherwise approved by the contracting officer. Such a requirement is consistent with OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, which states that agencies have the responsibility to notify individuals whose PII or SPII may have been compromised without unreasonable delay. In the past, this notification has often been delayed while detailed forensic analysis and contract compliance inspections are occurring. Under this new provision, notification and credit monitoring, when appropriate, will occur more rapidly as it is not dependent upon any determination of contractor fault or noncompliance.

The content and method of any notification sent by a contractor must be coordinated with and approved by the contracting officer. At a minimum, this notification must include: a brief description of the incident; a description of the types of PII or SPII involved; a statement as to whether the PII or SPII was encrypted or protected by other means; steps individuals may take to protect themselves; what the contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and information identifying who individuals may contact for additional information. Such notification is consistent with the "openness principle" of the Privacy Act which calls for agencies to inform individuals about how

their information is being accessed and used, and may help individuals mitigate the potential harms resulting from an incident.

Provision of Credit Protection to Impacted Individuals

Proposed clause *Safeguarding of Controlled Unclassified Information* requires contractors to provide credit monitoring services, including call center services to any individual whose PII or SPII was under the control of the contractor, or resided in the information system, at the time of the incident for a period beginning on the date of the incident and extending not less than 18 months from the date the individual is notified when directed by the contracting officer. Credit monitoring services can be particularly beneficial to the affected public as they can assist individuals in the early detection of identity theft as well as notify individuals of changes that appear in their credit report, such as creation of new accounts, changes to their existing accounts or personal information, or new inquiries for credit. Such notification affords individuals the opportunity to take steps to minimize any harm associated with unauthorized or fraudulent activity.

Incident Reporting

Proposed clause *Safeguarding of Controlled Unclassified Information* requires contractors and subcontractors to report all known or suspected incidents to the Component SOC. If the Component SOC is not available, the report shall be made to the DHS Enterprise SOC. While such a requirement is not new for DHS, compliance with this requirement is critical. The mission of DHS is unique in that we, through the National Protection and Programs Directorate's Office of Cybersecurity and Communications, are also responsible for the identification and sharing of cyber threat

indicators. These cyber threat indicators and defensive measures are shared among federal and non-federal entities consistent with the need to protect information systems from cybersecurity threats, mitigate cybersecurity threats, and comply with any other applicable provisions of law authorized by the Cybersecurity Information Sharing Act of 2015. Because of this mission requirement, DHS is not only concerned with actors who are successful in breaching our defenses, we are also concerned with attempts to breach those defenses. Knowledge of these attempts enables us to perform any necessary investigations and determine/establish new procedures to strengthen our defenses and prevent them from becoming successful. This information is then in turn shared with the interagency and non-Federal entities to enable them to take the necessary measures to be able to defend against similar attacks.

Improved Incident Response Time

Previously contractors were not consistently provided with specific incident reporting timelines. As such, the timeliness of incident reporting was determined by the contractor. Standardizing incident reporting timelines through proposed clause *Safeguarding of Controlled Unclassified Information* ensures timely incident reporting. Timely reporting of incidents is critical to prevent the impact of the incident from expanding, ensure incident response and mitigation activities are undertaken quickly, and ensure individuals are timely notified of the possible or actual compromise of their personally identifiable information and offered credit monitoring services when applicable.

IV. Regulatory Flexibility Act

DHS expects this proposed rule may have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq*. Therefore, an Initial Regulatory Flexibility Analysis (IRFA) has been prepared consistent with 5 U.S.C. 603, and is summarized as follows:

1. Description of the reasons why action by the agency is being considered.

Cybersecurity has been identified as one of the most serious economic and national security challenges our nation faces. The frequency of cyber-attacks, including attempts to gain unauthorized access to CUI collected or maintained by or on behalf of an agency and information systems that collect, process, store, or transmit such information, has prompted the Government to expand its cybersecurity efforts across the Federal landscape. Part of the DHS mission is to protect the nation's cybersecurity and to coordinate responses to cyber-attacks and security vulnerabilities. As part of that mission, DHS is proposing to amend the HSAR to expand its current security measures for safeguarding CUI to include additional requirements for the safeguarding of CUI that is accessed by contractors, collected or maintained by contractors on behalf of the agency, and Federal information systems, which includes contractor information systems operating on behalf of the Government, that collect, process, store or transmit CUI. These proposed revisions to the HSAR are necessary to ensure the integrity, confidentiality, and availability of CUI.

2. Succinct statement of the objectives of, and legal basis for, the rule.

The objective of this rule is to expand on existing Departmental IT security requirements. These existing IT security requirements are provided in the clause at

HSAR 3052.204-70, Security Requirements for Unclassified Information Technology Resources, and applicable DHS policy and guidance. The existing clause is more narrowly focused on information systems connected to a DHS network or operated by a contractor for DHS. This rule proposes to remove the existing clause and provide a new expanded clause. Unlike the existing clause, this proposed rule extends the scope to require that CUI be safeguarded wherever such information resides, including government-owned and operated information systems, government-owned and contractor operated information systems, contractor-owned and/or operated information systems operating on behalf of the Government, and any situation where contractor and/or subcontractor employees may have access to CUI consistent with the requirements of FISMA. This proposed rule also establishes uniform incident reporting and response activities that contractors and subcontractors must comply with in the event of an incident. The proposed rule also requires contractors and subcontractors have in place procedures and the capability to notify and provide credit monitoring services to any individual whose Personally Identifiable Information (PII) or Sensitive PII (SPII) was under the control of the contractor, or resided in the information system, at the time of the incident. Additionally, this proposed rule requires contractors and subcontractors to certify and confirm the sanitization of Government and Government-Activity related files and information. These collective measures will help DHS mitigate information security risks related to information as well as gather information for future improvements in information security policy.

The requirement to safeguard CUI is specified in the Federal Information Security Modernization Act of 2014 (44 U.S.C. 3551, *et seq.*), OMB Circular A-130, *Managing*

Information as a Strategic Resource, relevant National Institutes of Standards and Technology (NIST) guidance, Executive Order 13556, *Controlled Unclassified Information* and its implementing regulation at 32 CFR Part 2002, and various OMB Memoranda, to include: M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information;* M-14-03, *Enhancing the Security of Federal Information and Information Systems*; and Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management and Guidance on Federal Information Security and Privacy Management Requirements as identified in various OMB Memoranda.

3. Description of and, where feasible, estimate of the number of small entities to which the rule will apply.

This rule will apply to DHS contractors that require access to CUI, collect or maintain CUI on behalf of the Government, or operate Federal information systems, which includes contractor information systems operating on behalf of the agency, that collect, process, store or transmit CUI.

For Fiscal Year (FY) 2014, DHS awarded nearly 13,000 new contract awards to large and small businesses, with over 35 percent of all contracts awarded to small businesses. The estimate of the number of small entities to which the proposed rule will apply was established by reviewing FPDS data for FY 2014, internal DHS contract data, experience with similar safeguarding requirements used in certain DHS contracts, and the most likely applicable Product and Service Codes (PSCs). The data review identified 2,525 unique vendors were awarded contracts under the most likely applicable PSCs in FY 2014, including small and large businesses. However, not all contractors awarded

contracts under the most likely applicable PSCs will be subject to proposed clause *Safeguarding of Controlled Unclassified Information*. A number of factors determine the applicability of the proposed clause and would require analysis on a case-by-case basis. Further, the proposed clause is separated by those entities that are granted access to CUI but information systems will not be operated on behalf of the agency to collect, process, store or transmit CUI, and those that are required to meet the Authority to Operate (ATO) requirements because information systems will be used to collect, process, store or transmit CUI on behalf of the agency. Based on the data reviewed, the estimated number of annual respondents subject to the *Safeguarding of Controlled Unclassified Information* clause is estimated at 822 respondents. The proposed revision to the HSAR includes a flow-down provision that applies to subcontractors. However, DHS does not believe this requirement will add to the estimated number of respondents when an ATO is required because it is anticipated that a single information system will be used to collect, process, store, or transmit CUI in most instances. A review of DHS historical data shows that at least 35 percent of new contracts are awarded to small businesses. Therefore, it is assumed that 35 percent of the projected annual number of respondents will also be small businesses, or approximately 288 respondents.

Although the proposed HSAR clause is new, DHS contractors are currently required to comply with Departmental IT security policy and guidance. It is assumed that the average DHS IT services contractor covered by this clause will a have high operational security readiness posture. However, the requirements of the proposed clause have been expanded to include professional services contractors that have access to CUI, collect or maintain CUI on behalf of the Government, and/or operate Federal information

systems, including contractor information systems operating on behalf of the agency, that collect, process, store or transmit CUI to perform the requirements of their contract(s). While these contractors may not have the same operational security readiness posture of the average DHS IT services contractor, the expansion and implementation of these safeguarding requirements is necessary to further reduce risks and potential vulnerabilities.

4. Description of projected reporting, recordkeeping, and other compliance requirements of the rule, including an estimate of the classes of small entities which will be subject to the requirement and the type of professional skills necessary.

Reporting and recordkeeping requirements include those requirements necessary to ensure adequate security controls are in place when contractor and/or subcontractor employees will have access to sensitive CUI, collect or maintain CUI on behalf of the Government, and/or operate Federal information systems, which includes contractor information systems operating on behalf of the agency, that are used to collect, process, store, or transmit CUI. The reporting and recordkeeping requirements vary depending on if an Authority to Operate (ATO) is required. If an ATO is not required, the reporting and recordkeeping requirements include: Incident Reporting, Notification (if the incident involves PII/SPII), Credit Monitoring (if the incident involves PII/SPII), and Certification of Sanitization. If an ATO is required, the reporting and recordkeeping requirements include: Incident Reporting, Notification (if the incident involves PII/SPII), Credit Monitoring (if the incident involves PII/SPII), Certification of Sanitization, Security Authorization Package, Independent Assessment, Renewal of ATO, and Federal Reporting and Continuous Monitoring.

Typical contract awards that may include the requirement for access to CUI include contracts awards with a PSC of "D" Automatic Data Processing and Telecommunication and "R" Professional, Administrative and Management Support. However, this is not an all-inclusive list. Additional PSCs will be added and projections will be adjusted as additional data becomes available through HSAR clause implementation. This continued process will assist in validating future projections. It is estimated that the average contractor will utilize a mid-level manager with IT expertise to ensure compliance with the requirements of this rule.

5. Identification, to the extent practicable, of all relevant Federal rules which may duplicate, overlap, or conflict with the rule.

There are no rules that duplicate, overlap or conflict with this rule.

6. Description of any significant alternatives to the rule which accomplish the stated objectives of applicable statutes and which minimize any significant economic impact of the rule on small entities.

No significant alternatives were identified that would accomplish the stated objectives of the rule. The information security requirements associated with this rule are not geared towards a type of contractor; the requirements are based on the sensitivity of the information, the impact on the program, the Government and security in the event CUI is breached. That standard would not vary based on the size of the entity.

DHS will be submitting a copy of the IRFA to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the IRFA may be obtained from the point of contact specified herein. DHS invites comments from small business concerns and other interested parties on the expected impact of this rule on small entities.

DHS will also consider comments from small entities concerning the existing regulations in subparts affected by this rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610, *et seq*. (HSAR Case 2015-001), in correspondence.

V. Paperwork Reduction Act

The Paperwork Reduction Act (44 U.S.C. chapter 35) applies. The proposed rule contains information collection requirements. Accordingly, DHS will be submitting a request for approval of a new information collection requirement concerning this rule to the Office of Management and Budget under 44 U.S.C. 3501, *et seq*.

The collection requirements for this rule are based on a new HSAR clause, 3052.204-7X *Safeguarding of Controlled Unclassified Information*.

A. The average public reporting burden for this collection of information is estimated to be approximately 50 hours per response to comply with the requirements, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. This average is based on an estimated 36 hours per response to comply with the requirements when an ATO **is not** required an estimated 120 hours to comply with the requirements when an ATO **is** required (i.e., when a contractor is required to submit Security Authorization (SA) package). Security Authorization package consists of the following: Security Plan, Security Assessment Report, Plan of Action and Milestones, Security Control Assessor Transmittal Letter (documents the Security Control Assessor's recommendation (i.e., Authorization to Operate or Denial to Operate), and any supplemental information requested by the Government (e.g., Contingency Plan, final

Risk Assessment, Configuration Management Plan, Standard Operating Procedures, Concept of Operations). Additional requirements include an Independent Assessment, Security Review, Renewal of the ATO which is required every three years, and Federal Reporting and Continuous Monitoring Requirements.

The total annual projected number of responses per respondent is estimated at 1. Based on aforementioned information the annual total burden hours are estimated as follows:

Title: Homeland Security Acquisition Regulation: Safeguarding of Controlled Unclassified Information.

Type of Request: New Collection.

Total Number of Respondents: 822

Responses per Respondent: 1

Annual Responses: 822

Average Burden per Response: Approximately 50

Annual Burden Hours: Approximately 41,100

Needs and Uses: DHS needs the information required by 3052.204-7X to implement the requirements for safeguarding against unauthorized contractor disclosure and inappropriate use of CUI that contractors and subcontractors may have access to during the course of contract performance.

Affected Public: Businesses or other for-profit institutions.

Respondent's Obligation: Required to obtain or retain benefits.

Frequency: On occasion.

B. Request for Comments Regarding Paperwork Burden

You may submit comments identified by DHS docket number [DHS-2017-0006], including suggestions for reducing this burden, not later than [insert date 60 days after publication in the FEDERAL REGISTER] using any one of the following methods:

(1) Via the internet at Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

(2) Via email to the Department of Homeland Security, Office of the Chief Procurement Officer, at *HSAR@hq.dhs.gov*.

Public comments are particularly invited on: whether this collection of information is necessary for the proper performance of functions of the HSAR, and will have practical utility; whether our estimate of the public burden of this collection of information is accurate, and based on valid assumptions and methodology; ways to enhance the quality, utility, and clarity of the information to be collected; and ways in which we can minimize the burden of the collection of information on those who are to respond, through the use of appropriate technological collection techniques or other forms of information technology.

Requesters may obtain a copy of the supporting statement from the Department of Homeland Security, Office of the Chief Procurement Officer, Acquisition Policy and Legislation, via email to *HSAR@hq.dhs.gov*. Please cite OMB Control No. 1600-0023, Safeguarding of Controlled Unclassified Information, in all correspondence.

List of Subjects in 48 CFR Parts 3001, 3002, 3004 and 3052

Government procurement.

Therefore, DHS proposes to amend 48 CFR parts 3001, 3002, 3004 and 3052 as follows:

1. The authority citation for 48 CFR parts 3001, 3002, 3004 and 3052 is revised to read as follows:

Authority: 5 U.S.C. 301-302, 41 U.S.C. 1707, 41 U.S.C. 1702, 41 U.S.C. 1303(a)(2), 48 CFR part 1, subpart 1.3, and DHS Delegation Number 0702.

PART 3001—FEDERAL ACQUISITION REGUALTIONS SYSTEM

2. In section 3001.106 amend paragraph (a) by adding a new OMB Control Number as follows:

3001.106 OMB Approval under the Paperwork Reduction Act.

(a) * * *

OMB Control No. 1600-0023 (Safeguarding of Controlled Unclassified Information)

* * * * *

PART 3002--DEFINITIONS OF WORDS AND TERMS

3. Amend section 3002.101 by adding, in alphabetical order, the definitions of "Adequate Security," "Controlled Unclassified Information (CUI)," "Federal Information," "Federal Information System," "Handling," "Information Resources," "Information Security," and "Information System" to read as follows:

"Adequate Security" means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

*****

"Controlled Unclassified Information (CUI)" is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. Within the context of DHS, this includes such information which, if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in Title 6, Code of Federal Regulations, part 27 "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(3) Sensitive Security Information (SSI) as defined in Title 49, Code of Federal Regulations, part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee) to include DHS MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2010.1, "SSI Program";

(4) Homeland Security Agreement Information means information DHS receives pursuant to an agreement with state, local, tribal, territorial, and private sector partners that is required to be protected by that agreement. DHS receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Security Act;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information DHS receives pursuant to an information sharing agreement or arrangement, with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign

private or non-governmental organization, that is required by that agreement or arrangement to be protected;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) DHS information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526, will be classified as appropriate;

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means information that could constitute an indicator of U.S. Government intentions, capabilities, operations, or activities or otherwise threaten operations security;

(9) Personnel Security Information means information that could result in physical risk to DHS personnel or other individuals that DHS is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact

analysis studies, and certification and accreditation documentation;

(11) Privacy Information, which includes information referred to as Personally Identifiable Information. Personally Identifiable Information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual; and

(12) Sensitive Personally Identifiable Information (SPII) is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements.

(i) Examples of stand-alone PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan.

(ii) Additional examples of SPII include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits)

(B) Date of birth (month, day, and year)

(C) Citizenship or immigration status

(D) Ethnic or religious affiliation

(E) Sexual orientation

(F) Criminal history

(G) Medical information

(H) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

(iii) Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

"Federal Information" means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

"Federal Information System" means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.

"Handling" means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.

*****

"Information Resources" means information and related resources, such as personnel, equipment, funds, and information technology.

"Information Security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) availability, which means ensuring timely and reliable access to and use of information.

"Information System" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

*****

PART 3004--ADMINISTRATIVE MATTERS

4. Revise subpart 3004.4 to read as follows:

Subpart 3004.4 Safeguarding Classified and Controlled Unclassified Information within Industry

3004.470 Security requirements for access to unclassified facilities, information resources, and controlled unclassified information.

3004.470-1 Scope.

3004.470-2 Definitions.

3004.470-3 Policy.

3004.470-4 Contract Clauses.

3004.470-1 Scope.

This section implements DHS policies for assuring adequate security of unclassified facilities, information resources, and controlled unclassified information (CUI) during the acquisition lifecycle.

3004.470-2 Definitions.

As used in this subpart—

"Incident" means an occurrence that—

(1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

3004.470-3 Policy.

(a) DHS requires that CUI be safeguarded wherever such information resides. This includes government-owned and operated information systems, government-owned and contractor operated information systems, contractor-owned and/or operated information systems operating on behalf of the agency, and any situation where contractor and/or subcontractor employees may have access to CUI. There are several Department policies and procedures (accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors) which also address the safeguarding of CUI. Compliance with these policies and procedures, as amended, is required.

(b) DHS requires contractor employees that require recurring access to Government facilities or access to CUI to complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine fitness. Department policies and procedures that address contractor employee

fitness are contained in Instruction Handbook Number 121-01-007, The Department of Homeland Security Personnel Suitability and Security Program. Compliance with these policies and procedures, as amended, is required.

3004.470-4 Contract Clauses.

(a) Contracting officers shall insert the basic clause at (HSAR) 48 CFR 3052.204-71, Contractor Employee Access, in solicitations and contracts when contractor and/or subcontractor employees require recurring access to Government facilities or access to CUI. Contracting officers shall insert the basic clause with its Alternate I for acquisitions requiring contractor access to Government information resources. For acquisitions in which contractor and/or subcontractor employees will not have access to Government information resources, but the Department has determined contractor and/or subcontractor employee access to CUI or Government facilities must be limited to U.S. citizens and lawful permanent residents, the contracting officer shall insert the clause with its Alternate II. Neither the basic clause nor its alternates shall be used unless contractor and/or subcontractor employees will require recurring access to Government facilities or access to CUI. Neither the basic clause nor its alternates should ordinarily be used in contracts with educational institutions.

(b) Contracting officers shall insert the clause at (HSAR) 48 CFR 3052.204-7X, Safeguarding of Controlled Unclassified Information, in solicitations and contracts where:

(1) Contractor and/or subcontractor employees will have access to CUI;

(2) CUI will be collected or maintained on behalf of the agency; or

(3) Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI.

(c) If the clauses prescribed in subsections (a) and/or (b) are included in a prime contract, the prime contractor shall include the clauses in subsections (a) and/or (b), in its contract(s) with subcontractors. If a subcontract includes the clauses prescribed in subsections (a) and /or (b) and the subcontractor has contracts with lower-tier subcontractors, the lower-tier subcontracts shall include the clauses in subsections (a) and/or (b).

PART 3052—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

Section 3052.204-70 [Removed and Reserved].

5. Remove and reserve section 3052.204-70.

6. Add section 3052.204-7X to read as follows:

3052.204-7X Safeguarding of Controlled Unclassified Information.

As prescribed in (HSAR) 48 CFR 3004.470-4(b), insert the following clause:

SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION

(DATE)

(a) *Definitions*. As used in this clause—

"Adequate Security" means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide

appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

"Controlled Unclassified Information (CUI)" is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. Within the context of DHS, this includes such information which, if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals. This definition includes the following CUI categories and subcategories of information:

(i) Chemical-terrorism Vulnerability Information (CVI) as defined in Title 6, Code of Federal Regulations, part 27 "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(ii) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the

Department of Homeland Security (including the PCII Program Manager or his/her designee);

(iii) Sensitive Security Information (SSI) as defined in Title 49, Code of Federal Regulations, part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee) to include DHS MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2010.1, "SSI Program";

(iv) Homeland Security Agreement Information means information DHS receives pursuant to an agreement with state, local, tribal, territorial, and private sector partners that is required to be protected by that agreement. DHS receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Security Act;

(v) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(vi) International Agreement Information means information DHS receives pursuant to an information sharing agreement or arrangement with a foreign government,

an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization, that is required by that agreement or arrangement to be protected;

(vii) Information Systems Vulnerability Information (ISVI) means:

(A) DHS information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526, will be classified as appropriate;

(B) Information regarding developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(viii) Operations Security Information means information that could constitute an indicator of U.S. Government intentions, capabilities, operations, or activities or otherwise threaten operations security;

(ix) Personnel Security Information means information that could result in physical risk to DHS personnel or other individuals that DHS is responsible for protecting;

(x) Physical Security Information means reviews or reports illustrating or disclosing

facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property,. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(xi) Privacy Information, which includes information referred to as Personally Identifiable Information (PII). PII means information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and

(xii) Sensitive Personally Identifiable Information (SPII) is a subset of PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements.

(A) Examples of stand-alone SPII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan.

(B) Additional examples of SPII include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(*1*) Truncated SSN (such as last 4 digits)

(*2*) Date of birth (month, day, and year)

(*3*) Citizenship or immigration status

(*4*) Ethnic or religious affiliation

(*5*) Sexual orientation

(*6*) Criminal history

(*7*) Medical information

(*8*) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

(C) Other PII may be SPII depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not SPII.

"Federal information" means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

"Federal information system" means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.

"Handling" means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

"Incident" means an occurrence that—

(i) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(ii) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

"Information Resources" means information and related resources, such as personnel, equipment, funds, and information technology.

"Information Security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(i) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(ii) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(iii)availability, which means ensuring timely and reliable access to and use of information.

"Information System" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(b) *Handling of Controlled Unclassified Information.*

(1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*.

(2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.

(3) The Contractor shall not maintain SPII in its invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions. It is acceptable to maintain in these systems the names, titles and contact information for the Contracting Officer's Representative (COR) or other Government personnel associated with the administration of the contract, as needed.

(4) Any Government data provided, developed , obtained under the contract, or otherwise under the control of the contractor, shall not become part of the bankruptcy estate in the event a contractor and/or subcontractor enters into bankruptcy proceedings.

(c) *Authority to Operate*. This subsection is applicable only to Federal information systems, which includes contractor information systems operating on behalf of the agency. The Contractor shall not collect, process, store or transmit CUI within a Federal information system until an Authority to Operate (ATO) has been accepted and signed by the Component or Headquarters CIO, or designee. Once the ATO has been accepted and signed by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's acceptance of

the ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) Complete the Security Authorization process. The Security Authorization (SA) process shall proceed according to *DHS Sensitive Systems Policy Directive 4300A* (Version 12.0, September 25, 2015), or any successor publication; *DHS 4300A Sensitive Systems Handbook* (Version 12.0, November 15, 2015), or any successor publication; and the *Security Authorization Process Guide* including templates. These policies and templates are accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*.

(i) *Security Authorization Package*. SA package shall be developed using the Government provided Requirements Traceability Matrix and SA templates. SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

(ii) *Independent Assessment*. Contractors shall have an independent third party validate the security and privacy controls in place for the information system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations* accessible at *http://csrc.nist.gov/publications/PubsSPs.html*. The Contractor shall address all deficiencies before submitting the SA package to the COR for acceptance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

(i) Updating the SA package in the DHS Information Assurance Compliance System; or

(ii) Submitting the updated SA package directly to the COR.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are

being implemented and enforced. The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford access to DHS, the Office of the Inspector General, other Government organizations, and contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Federal Reporting and Continuous Monitoring Requirements.* Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. The plan is updated on an annual basis. Annual,

quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within three (3) business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than one year from the date the data is created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from Government tools and infrastructure.

(d) *Incident Reporting Requirements.*

(1) All known or suspected incidents shall be reported to the Component Security Operations Center (SOC) in accordance with *4300A Sensitive Systems Handbook Attachment F Incident Response*. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting to the Component or DHS Enterprise SOC. All known or suspected incidents involving PII or SPII shall be reported within one hour of discovery. All other incidents shall be reported within eight hours of discovery.

(2) The Contractor shall not include any CUI in the subject or body of any e-mail. The Contractor shall transmit CUI using *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods, accessible at *http://csrc.nist.gov/groups/STM/cmvp/standards.html*, to protect CUI in attachments to email. Passwords shall not be communicated in the same email as the attachment.

(3) An incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for CUI, or has otherwise failed to meet the requirements of the contract.

(4) If an incident involves PII or SPII, in addition to the incident reporting guidelines in *4300A Sensitive Systems Handbook Attachment F Incident Response*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);

(ii) Contract numbers affected unless all contracts by the company are affected;

(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);

(v) Contracting Officer POC (address, telephone, email);

(vi) Contract clearance level;

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;

(viii) Government programs, platforms or systems involved;

(ix) Location(s) of incident;

(x) Date and time the incident was discovered;

(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;

(xii) Description of the Government PII or SPII contained within the system; and

(xiii) Any additional information relevant to the incident.

(e) *Incident Response Requirements.*

(1) All determinations by the Department related to incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,

(ii) Investigations,

(iii) Forensic reviews,

(iv) Data analyses and processing, and

(v) Revocation of the Authority to Operate.

(4) The contractor shall preserve and protect images of known affected information systems identified in paragraph (b) of this section and all relevant monitoring/packet capture data for at least 90 days from submission of the incident report to allow DHS to request the media or decline interest.

(5) The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(f) *PII and SPII Notification Requirements.* This subsection is only applicable when an incident involves PII/ SPII.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII and/or SPII was under the control of the Contractor or resided in the information system at the time of the incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer utilizing the DHS Privacy Incident Handling Guidance accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail,

electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;

(ii) A description of the types of PII or SPII involved;

(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

(iv) Steps individuals may take to protect themselves;

(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and

(vi) Information identifying who individuals may contact for additional information.

(g) *Credit Monitoring Requirements.* This subsection is only applicable when an incident involves PII/ SPII. In the event that an incident involves PII or SPII, the Contractor may be directed by the Contracting Officer to:

(1) Provide notification to affected individuals as described in paragraph (f).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the Contractor or resided in the information system at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;

(ii) Daily customer service;

(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts.

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;

(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(h) *Certificate of Sanitization of Government and Government-Activity-Related Files and Information.* Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI

to DHS and/or destroy it physically and/or logically as identified in the contract. Destruction shall conform to the guidelines for media sanitization contained in *NIST SP-800-88, Guidelines for Media Sanitization*. The Contractor shall certify and confirm the sanitization of all Government and Government-Activity related files and information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in *NIST Special Publication 800-88, Guidelines for Media Sanitization, Appendix G*.

(i) *Other Reporting Requirements.* Incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable U.S. Government statutory or regulatory requirements.

(j) *Subcontracts.* The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower-tier subcontracts.

(End of clause)

7. Amend paragraph (b) of section 3052.212-70 to remove 3052.204-70 Security Requirements for Unclassified Information Technology Resources; add Alternate II of 3052.204-71, Contractor Employee Access; and add 3052.204-7X, Safeguarding of Controlled Unclassified Information, as follows:

3052.212-70 Contract terms and conditions applicable to DHS acquisition of commercial items.

CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (DATE)

* * * * *

(b) * * *

____3052.204-71 Contractor Employee Access.

____Alternate I

____Alternate II

* * *

____3052.204-7X Safeguarding of Controlled Unclassified Information.

Soraya Correa

Chief Procurement Officer, Department of Homeland Security

[FR Doc. 2017-00758 Filed: 1/18/2017 8:45 am; Publication Date: 1/19/2017]